B. AMENDMENTS TO THE CLAIMS

Claim 1 (Currently amended) A method of establishing a secure communication path between two computer systems comprising:

creating a communication path to exchange ~~data such as~~ data, including identification data and digital certification ~~data~~ data, between the two systems;

determining, based on the identification data, whether to confirm that the digital certification data has not been revoked; and

creating a secure communication path, without confirming that the digital certification data has not been revoked if it is determined ~~the digital certification data~~ that it should not be confirmed that the digital certification data has not been revoked, or after confirming that the digital certification data has not been revoked if it is determined ~~that the digital certification data~~ it should be confirmed that the digital certification data has not been revoked.

Claim 2 (Currently amended) The method as described in claim 1 wherein the determining step includes the step of consulting an internal table, the internal table including identification data of all computer systems ~~whose digital certification need not be confirmed~~ for which it is not necessary to confirm that digital certification data has not been revoked.

Claim 3 (Original) The method as described in claim 2 wherein the two computer systems include a local and a remote computer system, the exchanged data further including one or more authentication proposals from the local computer system and a selected authentication proposal from the remote system.

Claim 4 (Currently amended) The method as described in claim 1 further comprising:

selecting an access method in response to determining to confirm whether the digital certification data has not been revoked; and

invoking the selected access method.

Claim 5 (Original) The method as described in claim 1 further comprising:

selecting a local-remote pair from an endpoints table corresponding to the computer systems;

selecting a policy from a policy table based on the selected local-remote pair, the policy including one or more access methods; and

transmitting one or more security proposals corresponding to the selected policy to the remote computer system.

Claim 6 (Original) The method as described in claim 1 further comprising:

receiving a remote digital certificate from the other computer system; and

verifying that a signing certificate included in the remote digital certificate corresponds to a certification authority.

Claim 7 (Original) The method as described in claim 1 further comprising:

digitally signing a message using a private key corresponding to one of the computer systems; and

sending the signed message to the other computer system.

Claim 8 (Currently amended) An information handling system comprising:

one or more processors;

a memory accessible by the processors;

a nonvolatile storage accessible by the processors;

a network interface connecting the information handling system to a computer network; and

a network security tool to create a secure path between computer systems, the network security tool including:

means for creating a non-secure communication path to exchange ~~data such as~~ data, including identification data and digital certification ~~data~~ data, between the two systems;

means for determining, based on the identification data, whether to confirm that the digital certification data has not been revoked; and

means for creating a secure communication path, without confirming that the digital certification data has not been revoked if it is determined ~~the digital certification data~~ that it should not be confirmed that the digital certification data has not been revoked, or after confirming that the digital certification data has not been revoked if it is determined that ~~the digital certification data~~ it should be confirmed that the digital certification data has not been revoked.

Claim 9 (Currently amended) The information handling system as described in claim 8 wherein the means for determining includes means for consulting an internal table, the internal table including identification data of all computer systems ~~whose digital certification need not be confirmed~~ for which it is not necessary to confirm that digital certification data has not been revoked.

Claim 10 (Original) The information handling system as described in claim 9 wherein the two computer systems include a local and a remote computer system, the exchanged data further including one or more authentication proposals from the local computer system and a selected authentication proposal from the remote system.

Claim 11 (Currently amended) The information handling system as described in claim 8 further comprising:

means for selecting an access method in response to determining to confirm that the digital certification data has not been revoked; and

means for invoking the selected access method.

Claim 12 (Original) The information handling system as described in claim 8 further comprising:

means for selecting a local-remote pair from an endpoints table corresponding to the computer systems;

means for selecting a policy from a policy table based on the selected local-remote pair, the policy including one or more access methods; and

means for transmitting one or more security proposals corresponding to the selected policy to the remote computer system.

Claim 13 (Original) The information handling system as described in claim 8 further comprising:

means for receiving a remote digital certificate from the other computer system; and

means for verifying that a signing certificate included in the remote digital certificate corresponds to a certification authority.

Claim 14 (Currently amended) A computer program product stored on a computer operable medium for providing one or more secure connections from a computer system, said computer program product comprising:

means for creating a non-secure communication path to exchange ~~data such as~~ data, including identification data and digital certification ~~data~~ data, between the two systems;

means for determining, based on the identification data, whether to confirm that the digital certification data has not been revoked; and

means for creating a secure communication path, without confirming the digital certification data if it is determined ~~the digital certification data~~ that it should not be confirmed that the digital certification data has not been revoked, or after confirming the digital certification data if it is determined that ~~the digital certification data~~ it should be confirmed that the digital certification data has not been revoked.

Claim 15 (Currently amended) The computer program product as described in claim 14 wherein the means for determining includes means for consulting an internal table, the internal table including identification data of all computer systems ~~whose digital certification need not be confirmed~~ for which it is not necessary to confirm that digital certification data has not been revoked.

Claim 16 (Original) The computer program product as described in claim 15 wherein the two computer systems include a local and a remote computer system, the exchanged data further including one or more authentication proposals from the local computer system and a selected authentication proposal from the remote system.

Claim 17 (Currently amended) The computer program product as described in claim 14 further comprising:

means for selecting an access method in response to determining to confirm that the digital certification data has not been revoked; and

means for invoking the selected access method.

Claim 18 (Original) The computer program product as described in claim 14 further comprising:

means for selecting a local-remote pair from an endpoints table corresponding to the computer systems;

means for selecting a policy from a policy table based on the selected local-remote pair, the policy including one or more access methods; and

means for transmitting one or more security proposals corresponding to the selected policy to the remote computer system.

Claim 19 (Original) The computer program product as described in claim 14 further comprising:

means for receiving a remote digital certificate from the other computer system; and

means for verifying that a signing certificate included in the remote digital certificate corresponds to a certification authority.

Claim 20 (Original) The computer program product as described in claim 14 further comprising:

means for digitally signing a message using a private key corresponding to one of the computer systems; and

means for sending the signed message to the other computer system.

Claim 21 (New) A method of establishing a secure communication path between two computer systems comprising:

creating a communication path to exchange data, including identification data and digital certification data, between the two systems;

determining, based on the identification data, whether to confirm that the digital certification data has not been revoked, wherein the determining includes consulting an internal table, the internal table including identification data of all computer systems for which it is not necessary to confirm that certification data has not been revoked;

creating a secure communication path, without confirming that the digital certification data has not been revoked if it is determined that it should not be confirmed that the digital certification data has not been revoked, or after confirming that the digital certification data has not been revoked if it is determined that it should be confirmed that the digital certification data has not been revoked;

selecting a local-remote pair from an endpoints table corresponding to the computer systems;

selecting a policy from a policy table based on the selected local-remote pair, the policy including one or more access methods; and

transmitting one or more security proposals corresponding to the selected policy to the remote computer system.